UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,165	11/14/2001	Christopher Uhlik	15685P078C	5755

8791 7590 05/11/2007

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
AHMED, SALMAN	

ART UNIT	PAPER NUMBER
2616	

MAIL DATE	DELIVERY MODE
05/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

SK

Office Action Summary	Application No.	Applicant(s)	
	10/003,165	UHLIK ET AL.	
	Examiner	Art Unit	
	Salman Ahmed	2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *2/12/2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,6-9,12-19 and 25-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,6-9,12-19 and 25-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11/14/2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1, 2, 6-9, 12-19 and 25-28 are pending

Claims 3-5, 10, 11, and 20-24 are cancelled by the Applicant.

Claims 1, 2, 6-9, 12-19 and 25-28 are rejected.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

1. Claims 1, 6, 7, 12, 13 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chuah et al. (US PAT 6577644), hereinafter referred to as Chuah in

view of Ho et al. (US PAT PUB 2002/0116501), hereinafter referred to as Ho, and Akhtar et al. (US PAT 6769000), hereinafter referred to as Akhtar.

In regards to claim 1 Chuah teaches *a data networking protocol* (column 3 lines 1-2, PPP) *comprising: one or more control commands* (column 3 line 3, link-layer messages) *employed by a respective network element to establish and manage one or two simultaneous wireless communication session* (figure 4, multiple PPP links between Peer A and Peer B) *of a single wireless end user terminal* (column 1, lines 50-55, Multilink PPP is enhanced to provide for a more flexible quality of service (QoS) support in a wireless environment. In particular, and in accordance with the invention, multilink PPP is enhanced to enable a packet interface, or packet endpoint, to transmit a message to an opposite PPP peer, where the message identifies the number, and type, of classes on a particular PPP link). Chuah discloses the use of a Multilink PPP. Chuah in column 4 lines 5-30 and FIG. 4 illustrates use of the Non-Sharing QOS Option with standard Multilink PPP. Chuah teaches that for convenience, in FIG. 4 it is assumed that the transmitting peer is Peer A and the receiving peer is Peer B (transmitting and receiving from the point of view of negotiation, e.g., Peer A requests the Non-Sharing QoS option.) As noted above, the Non-sharing QoS option message allows a PPP peer to specify the number of classes to be carried on a particular link. For example, assumed a PPP peer first activates a link (link 1) using this Non-Sharing QoS option message and specifies that there will be two classes on link 1, namely classes 3 and 4. (That is, the NoCls field is set to 2, and the QoS Bitmap field is set to "00011000.") Then, the PPP peer subsequently activates 2 more links without enabling the Non-

sharing QoS option (i.e., no Non-Sharing QoS option message was included in the negotiation phase for these additional links). This means all PPP frames with class numbers 3 and 4 will be carried over link 1, the rest of the PPP frames will be segmented, or fragmented, (as is done in multilink PPP) and carried over the two remaining links (links 2 and 3) that were not negotiated with the Non-Sharing QoS option. Finally, it provides the ability to map packets from one or multiple IP sessions into one of the wireless link in the link bundle. In other words, a packet endpoint knows the exact types of the different classes that will be activated over any specific link. Examiner respectfully points out that from the above description it is understood that Chuah teaches multiple PPP links, multiple sessions and PPP that allows packets from some given sessions to be sent to one link and packets from other sessions to be sent to another link. As such, multiple PPP links between Peer A and Peer B carries multiple sessions between them.

Chuah does not explicitly teach *one or more mobility management attribute-value pair(s) (AVP), employed by the network element to define one or more parameters of the accompanying control command and to facilitate exchange of mobility information in the data network.*

Ho teaches (page 5 section 0075) AVP being used to encode control message types to exchange of mobility information.

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Chuah's system/method by incorporating the Ho's teachings of sending AVP via control command and to facilitate exchange of mobility

information. The motivation is that (as suggested by Chuah, column 1 lines 27-28) enhanced PPP provides robust and flexible quality of service (QoS) features in a network. Further motivation is that (as suggested by Ho, page 5, section 0075) Control messages 48 (see FIG. 2) are used in the efficient establishment maintenance, and tearing down of service tunnels, such as service tunnels 30-32. To maximize extensibility while still permitting interoperability, a uniform method for encoding control Message Types and bodies called Attribute Value pair (AVP) is used throughout L2TP.

In regards to claims 1, 6, 7, 12, and 13 Chuah in view of Ho, teach of using attribute-value pair for mobility management as described above.

In regards to claim 1 Chuah and Ho do not explicitly teach *facilitating secure mobility of wireless communication sessions.* In regards to claims 6, 7, 12 and 13 Chuah in view of Ho does not explicitly teach *authentication AVP during hand-off.* In regards to claims 12 and 13 Chuah, in view of Ho do not explicitly teach *mobility information comprises at least a portion of a communication session identifier that follows a communication session as it traverses through mobile communication link handoffs, the communication session identifier at least in part to implement mobility security features and communication session identifier is used to authenticate a mobile communication link handoff.*

In regards to claims 1, 6, 7, 12 and 13 Akhtar in the same field of endeavor teaches that IPM-L2-Address AVP (column 84 lines 15-20), carries the L2-Address of IPM Client connection. The AVP carries both Address and Data. The types of Addresses include, among others, 802.3 Address (0), 802.11 Address (1), IMSI (2), and

MIN (3). Akthar further teaches IPM-SMM-MN-Key AVP (column 84 lines 59-61) carries the shared secret key between Serving Mobility Manager and Mobile Node. This key is only valid for the session. In regards to claim 6 and 7 Akthar teaches (column 83 lines 5-7) that Integrity-Check-Value AVP is used for hop-by-hop message authentication and integrity.

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Chuah and Ho's system/method to incorporate Akhtar's teaching of deterministic element attribute-value pair (COOKIE AVP), random element attribute-value pair (K_n AVP) and authentication AVP. The motivation is that, (as suggested by Ho, page 5, section 0075) in L2TP protocol, AVP gives an advantage to maximize extensibility while still permitting interoperability. As such, necessary network parameters for session identification or authentication can be encoded in AVP for extensibility while still permitting interoperability.

In regards to claim 14, Chuah does not explicitly teach *attribute-value pairs comprise an extension of the Layer Two Tunneling Protocol (L2TP) and are employed to define one or more parameters of one or more existing L2TP control commands.*

In regards to claim 14 Ho teaches (page 5, section 0075) Control messages 48 (see FIG. 2) are used in the establishment maintenance, and tearing down of service tunnels, such as service tunnels 30-32. To maximize extensibility while still permitting interoperability, a uniform method for encoding control Message Types and bodies is used throughout L2TP. This encoding is called Attribute Value pair (AVP). An Attribute Value pair is defined as the variable length concatenation of unique attribute

(represented by an integer) and a value containing the actual value identified by the attribute.

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Chuah's system/method by incorporating the Ho's teachings of sending AVP via control command and to facilitate exchange of mobility information. The motivation is that (as suggested by Chuah, column 1 lines 27-28) enhanced PPP provides robust and flexible quality of service (QoS) features in a network. Further motivation is that (as suggested by Ho, page 5, section 0075) Control messages 48 (see FIG. 2) are used in the efficient establishment maintenance, and tearing down of service tunnels, such as service tunnels 30-32. To maximize extensibility while still permitting interoperability, a uniform method for encoding control Message Types and bodies called Attribute Value pair (AVP) is used throughout L2TP.

2. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chuah, Ho and Akhtar as applied to claim 1 above, and further in view of Chuah et al. (US PAT 6917600), hereinafter referred to as Chuah2.

In regards to claim 2, Chuah, Ho and Akhtar, teach of AVP being used in control command and to facilitate exchange of mobility information as described in the rejection of claim 1 above.

Chuah, Ho and Akhtar do not explicitly teach *the mobility management Attribute-value pairs include an attribute value pair denoting whether an incoming call request is a new call or a handoff.*

Chuah2 in the same field of endeavor teaches (column 12 lines 60-67 and column 13 lines 1-2) the steps of combining hand-off control messages (CCRQ, CCRP, and CCCN) with the tunnel configuration (establishment) control messages (SCCRQ, SCCRP, and SCCCN) and are, respectively, concurrently transmitted between LACs. So the messages can either be purely SCCRQ having a tunnel configuration (establishment) control part or SCCRQ with CCRQ having a hand-off part as well.

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify to modify Chuah, Ho and Akhtar's system/method by incorporating the method of sending establishment or handoff AVP via control command and to facilitate exchange of mobility information as taught by Chuah2. The motivation is that (as suggested by Ho, page 5, section 0075) Control messages 48 (see FIG. 2) are used in the establishment maintenance, and tearing down of service tunnels, such as service tunnels 30-32. To maximize extensibility while still permitting interoperability, a uniform method for encoding control Message Types and bodies is used throughout L2TP. This encoding is called Attribute Value pair (AVP). An Attribute Value pair is defined as the variable length concatenation of unique attribute (represented by an integer) and a value containing the actual value identified by the attribute.

3. Claims 15-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chuah in view of Akhtar.

In regards to claims 15-19 Chuah teaches *one or more control commands employed by a respective network element to establish and manage simultaneous*

wireless communication sessions (column 1, lines 50-55, Multilink PPP is enhanced to provide for a more flexible quality of service (QoS) support in a wireless environment. In particular, and in accordance with the invention, multilink PPP is enhanced to enable a packet interface, or packet endpoint, to transmit a message to an opposite PPP peer, where the message identifies the number, and type, of classes on a particular PPP link) *of a wireless subscriber unit* (column 1, lines 50-55, packet endpoint), *in a data network* (column 2 line 43, three new hand-off control messages, column 2 lines 10-11); *One or more mobility management attribute-value pair(s) (AVP) employed by the network element to define one or more parameters of the accompanying control command and to facilitate exchange of mobility information in the data network, wherein the mobility management attribute-value pair(s) include an attribute-value pair* (column 8 lines 4-11, additional Attribute Value Pairs (AVP) are defined for use in the L2TP control messages, hence, becoming mL2TP control messages. These additional AVPs are for supporting the multi-hop features and call transfer features). Chuah discloses the use of a Multilink PPP. Chuah in column 4 lines 5-30 and FIG. 4 illustrates use of the Non-Sharing QOS Option with standard Multilink PPP. Chuah teaches that for convenience, in FIG. 4 it is assumed that the transmitting peer is Peer A and the receiving peer is Peer B (transmitting and receiving from the point of view of negotiation, e.g., Peer A requests the Non-Sharing QoS option.) As noted above, the Non-sharing QoS option message allows a PPP peer to specify the number of classes to be carried on a particular link. For example, assumed a PPP peer first activates a link (link 1) using this Non-Sharing QoS option message and specifies that there will be two classes on link 1,

namely classes 3 and 4. (That is, the NoCls field is set to 2, and the QoS Bitmap field is set to "00011000.") Then, the PPP peer subsequently activates 2 more links without enabling the Non-sharing QoS option (i.e., no Non-Sharing QoS option message was included in the negotiation phase for these additional links). This means all PPP frames with class numbers 3 and 4 will be carried over link 1, the rest of the PPP frames will be segmented, or fragmented, (as is done in multilink PPP) and carried over the two remaining links (links 2 and 3) that were not negotiated with the Non-Sharing QoS option. Finally, it provides the ability to map packets from one or multiple IP sessions into one of the wireless link in the link bundle. In other words, a packet endpoint knows the exact types of the different classes that will be activated over any specific link. Examiner respectfully points out that from the above description it is understood that Chuah teaches multiple PPP links, multiple sessions and PPP that allows packets from some given sessions to be sent to one link and packets from other sessions to be sent to another link. As such, multiple PPP links between Peer A and Peer B carries multiple sessions between them.

Chuah does not explicitly teach *a deterministic element attribute-value pair (COOKIE AVP) or random element attribute-value pair (K_n AVP).*

Akhtar in the same field of endeavor teaches that IPM-L2-Address AVP (column 84 lines 15-20), carries the L2-Address of IPM Client connection. The AVP carries both Address and Data. The types of Addresses include, among others, 802.3 Address (0), 802.11 Address (1), IMSI (2), and MIN (3). Akthar further teaches IPM-SMM-MN-Key AVP (column 84 lines 59-61) carries the shared secret key between Serving Mobility

Manager and Mobile Node. This key is only valid for the session. In regards to claim 6 and 7 Akthar teaches (column 83 lines 5-7) that Integrity-Check-Value AVP is used for hop-by-hop message authentication and integrity.

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Chuah's system/method to incorporate Akhtar's teaching of deterministic element attribute-value pair (COOKIE AVP), random element attribute-value pair (K_n AVP) and authentication AVP. The motivation is that in L2TP protocol, AVP gives an advantage to maximize extensibility while still permitting interoperability, by using a uniform method for encoding message types and bodies. As such, necessary network parameters for session identification or authentication are encoded in AVP for extensibility while still permitting interoperability.

In regards to claim 19 Chuah teaches (column 12 lines 60-67 and column 13 lines 1-2) the steps of combining hand-off control messages (CCRQ, CCRP, and CCCN) with the tunnel configuration (establishment) control messages (SCCRQ, SCCRP, and SCCCN) and are, respectively, concurrently transmitted between LACs. So the messages can either be purely SCCRQ having a tunnel configuration (establishment) control part or SCCRQ with CCRQ having a hand-off part as well.

4. Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chuah, Ho and Akhtar, as applied to claim 1 above and further in view of Tummala et al. (US PAT 6915345), hereinafter referred to as Tummala.

In regards to claims 8 and 9 Chuah, Ho and Akhtar teach of using AVP to do authentication during network hops.

Chuah, Ho and Akhtar do not specifically teach *certificate AVP and validation from a third party certification agency or authority.*

Tummala in the same field of endeavor teaches (column 14 lines 33-38) that the encryption can be made using a shared secret or public keys, in the same manner as the Key AVPs returned by the AAAH in the Diameter Mobile IP Extensions when setting up the data security. If using PKI, the broker must be able to interface with a Certificate Authority (CA) or have those keys in storage.

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Chuah, Ho and Akhtar's system/method by incorporating Tummala's teaching of using security certificate in conjunction with certification authority. The motivation is that using security AVPs with security certificate in conjunction with certification authority or agency will enhance network security and prevent security breach.

5. Claims 25-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chuah in view of Ho, Akhtar and Abrol et al. (US PAT 7096261, hereinafter Abrol).

In regards to claim 25, Chuah teaches *receiving data transmissions for simultaneous wireless communication sessions* (figure 4, multiple PPP links between Peer A and Peer B), *a communications agent that employs one or more control commands* (column 3 line 3, link-layer messages) *to establish and manage*

simultaneous wireless communication sessions (column 1, lines 50-55, Multilink PPP is enhanced to provide for a more flexible quality of service (QoS) support in a wireless environment. In particular, and in accordance with the invention, multilink PPP is enhanced to enable a packet interface, or packet endpoint, to transmit a message to an opposite PPP peer, where the message identifies the number, and type, of classes on a particular PPP link). Chuah discloses the use of a Multilink PPP. Chuah in column 4 lines 5-30 and FIG. 4 illustrates use of the Non-Sharing QOS Option with standard Multilink PPP. Chuah teaches that for convenience, in FIG. 4 it is assumed that the transmitting peer is Peer A and the receiving peer is Peer B (transmitting and receiving from the point of view of negotiation, e.g., Peer A requests the Non-Sharing QoS option.) As noted above, the Non-sharing QoS option message allows a PPP peer to specify the number of classes to be carried on a particular link. For example, assumed a PPP peer first activates a link (link 1) using this Non-Sharing QoS option message and specifies that there will be two classes on link 1, namely classes 3 and 4. (That is, the NoCls field is set to 2, and the QoS Bitmap field is set to "00011000.") Then, the PPP peer subsequently activates 2 more links without enabling the Non-sharing QoS option (i.e., no Non-Sharing QoS option message was included in the negotiation phase for these additional links). This means all PPP frames with class numbers 3 and 4 will be carried over link 1, the rest of the PPP frames will be segmented, or fragmented, (as is done in multilink PPP) and carried over the two remaining links (links 2 and 3) that were not negotiated with the Non-Sharing QoS option. Finally, it provides the ability to map packets from one or multiple IP sessions into one of the wireless link in the link

bundle. In other words, a packet endpoint knows the exact types of the different classes that will be activated over any specific link. Examiner respectfully points out that from the above description it is understood that Chuah teaches multiple PPP links, multiple sessions and PPP that allows packets from some given sessions to be sent to one link and packets from other sessions to be sent to another link. As such, multiple PPP links between Peer A and Peer B carries multiple sessions between them.

Chuah does not explicitly teach *one or more mobility management attribute-value pair(s) (AVP), employed by the network element to define one or more parameters of the accompanying control command and to facilitate exchange of mobility information in the data network.*

Ho teaches (page 5 section 0075) AVP being used to encode control message types to exchange of mobility information.

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Chuah's system/method by incorporating Ho's teachings of sending AVP via control command and to facilitate exchange of mobility information. The motivation is that (as suggested by Chuah, column 1 lines 27-28) enhanced PPP provides robust and flexible quality of service (QoS) features in a network. Further motivation is that (as suggested by Ho, page 5, section 0075) Control messages 48 (see FIG. 2) are used in the efficient establishment maintenance, and tearing down of service tunnels, such as service tunnels 30-32. To maximize extensibility while still permitting interoperability, a uniform method for encoding control Message Types and bodies called Attribute Value pair (AVP) is used throughout L2TP.

In regards to claim 25 Chuah and Ho, teach using attribute-value pair for mobility management as described above.

Chuah and Ho do not explicitly teach *facilitating secure mobility of wireless communication sessions*.

Akhtar in the same field of endeavor teaches that IPM-L2-Address AVP (column 84 lines 15-20), carries the L2-Address of IPM Client connection. The AVP carries both Address and Data. The types of Addresses include, among others, 802.3 Address (0), 802.11 Address (1), IMSI (2), and MIN (3). Akthar further teaches IPM-SMM-MN-Key AVP (column 84 lines 59-61) carries the shared secret key between Serving Mobility Manager and Mobile Node. This key is only valid for the session. In regards to claim 6 and 7 Akthar teaches (column 83 lines 5-7) that Integrity-Check-Value AVP is used for hop-by-hop message authentication and integrity.

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Chuah and Ho's system/method to incorporate Akhtar's teaching of deterministic element attribute-value pair (COOKIE AVP), random element attribute-value pair (K_n AVP) and authentication AVP as suggested by Akhtar. The motivation is that (as suggested by Ho, page 5, section 0075) in L2TP protocol, AVP gives an advantage to maximize extensibility while still permitting interoperability, by using a uniform method for encoding message types and bodies. As such, necessary network parameters for session identification or authentication are encoded in AVP for extensibility while still permitting interoperability.

In regards to claim 25, Chuah, Ho and Akhtar do not explicitly teach *wireless end-user terminal, comprising: an antenna to receive data transmissions for simultaneous wireless communication sessions via a wireless modem coupled with the antenna.*

Abrol in the same field of endeavor teaches a wireless end-user terminal (FIG. 3 shows an exemplary mobile station (MS)), comprising: an antenna (Figure 3, antenna 308) to receive data transmissions via a wireless modem (Figure 3, a wireless modem 304) coupled with the antenna.

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Chuah, Ho and Akhtar's system/method by incorporating a wireless end-user terminal, comprising: an antenna to receive data transmissions for simultaneous wireless communication sessions via a wireless modem coupled with the antenna as suggested by Abrol. The motivation is that such components are essential for a mobile terminal and enables a the device to wirelessly communicate with other wireless elements in the network; thus making wireless communication a reality.

In regards to claim 26 Akhtar teaches *the mobility management attribute-value pair(s) include an authentication AVP* (IPM-SMM-MN-Key AVP in column 84 lines 59-61) *selectively invoked by one or more network elements participating in a point-to-point communication session to authenticate one or more network elements during a handoff of a communication session from one network element to another network element* (column 84 lines 15-20, IPM-L2-Address AVP, carries the L2-Address of IPM Client connection. The AVP carries both Address and Data. The types of Addresses include,

among others, 802.3 Address (0), 802.11 Address (1), IMSI (2), and MIN (3). Akthar further teaches IPM-SMM-MN-Key AVP (column 84 lines 59-61) carries the shared secret key between Serving Mobility Manager and Mobile Node. This key is only valid for the session. Akthar teaches (column 83 lines 5-7) that Integrity-Check-Value AVP is used for hop-by-hop message authentication and integrity).

In regards to claim 27 Akhtar teaches *the mobility information comprises at least a portion of a communication session identifier* (IPM-L2-Address AVP and IPM-SMM-MN-Key AVP) *that follows a communication session as it traverses through mobile communication link handoffs, the communication session identifier at least in part to implement mobility security features* (column 84 lines 15-20, IPM-L2-Address AVP, carries the L2-Address of IPM Client connection. The AVP carries both Address and Data. The types of Addresses include, among others, 802.3 Address (0), 802.11 Address (1), IMSI (2), and MIN (3). Akthar further teaches IPM-SMM-MN-Key AVP (column 84 lines 59-61) carries the shared secret key between Serving Mobility Manager and Mobile Node. This key is only valid for the session. Akthar teaches (column 83 lines 5-7) that Integrity-Check-Value AVP is used for hop-by-hop message authentication and integrity).

In regards to claim 28, Akhtar teaches *the communication session identifier is used to authenticate a mobile communication link handoff* (column 84 lines 15-20, IPM-L2-Address AVP, carries the L2-Address of IPM Client connection. The AVP carries both Address and Data. The types of Addresses include, among others, 802.3 Address (0), 802.11 Address (1), IMSI (2), and MIN (3)). Akthar further teaches IPM-SMM-MN-

Key AVP (column 84 lines 59-61) carries the shared secret key between Serving Mobility Manager and Mobile Node. This key is only valid for the session. Akthar teaches (column 83 lines 5-7) that Integrity-Check-Value AVP is used for hop-by-hop message authentication and integrity).

Response to Arguments

6. Applicant's arguments see pages 6-12 of the Remarks section, filed 2/12/2007, with respect to the rejection of claims 1, 2, 6-9, and 11-24 have been fully considered but they are not persuasive.

Claims 1, 6, 7, 11-14:

In regards to claim 1, Applicant argues (page 7 paragraph 1) that *Chuah only discusses Multilink PPP as a protocol used for physical links between physical endpoints; Multilink PPP is not a wireless protocol and the cited portion of Chuah does not discuss mobile nodes.* However, Examiner respectfully disagrees with such assertion. Chuah, does teach using Multilink PPP in a wireless as described in the rejection of claim 1 above. Specifically, Chuah clearly states in summary of the invention that (column 1, lines 50-55) Multilink PPP is enhanced to provide for a more flexible quality of service (QoS) support in a wireless environment. In particular, and in accordance with the invention, multilink PPP is enhanced to enable a packet interface, or packet endpoint (mobile node), to transmit a message to an opposite PPP peer, where the message identifies the number, and type, of classes on a particular PPP link.

Applicant argues (page 7 second paragraph) that *neither peer A nor peer B of Fig. 4 can be a wireless end-user terminal because peers A and B communicate via Multilink PPP, which, according to Chuah, requires that they are physically connected.* However, Examiner respectfully disagrees with the assertion. As mentioned earlier, Chuah's invention is for wireless communication in particular, as disclosed in the summary. Specifically, Chuah clearly states in summary of the invention that (column 1, lines 50-55) Multilink PPP is enhanced to provide for a more flexible quality of service (QoS) support in a wireless environment. In particular, and in accordance with the invention, multilink PPP is enhanced to enable a packet interface, or packet endpoint (mobile node), to transmit a message to an opposite PPP peer, where the message identifies the number, and type, of classes on a particular PPP link. Examiner further respectfully disagrees with the Applicant that physical connection cannot be wireless. Examiner submits that Physical Layer in OSI model is just not for wire line communication. The Physical Connection in Physical Layer of OSI model also equally applicable to wireless communication.

Examiner respectfully disagrees with the Applicant (page 8 paragraph 1) that Ho fails to cure the deficiencies of Chuah; as Chuah indeed does teach the cited alleged deficiencies as described above in the rejection of claim 1.

Examiner respectfully disagrees with the Applicant (page 8 paragraph 2) that Akhtar fails to cure the deficiencies of Chuah; as Chuah indeed does teach the cited alleged deficiencies as described above in the rejection of claim 1.

Claim 2:

Examiner respectfully disagrees with the Applicant (page 8-9 paragraphs 4-1) that Chuah2 fails to cure the deficiencies of Chuah, Ho and Akhtar; as Chuah indeed does teach the cited alleged deficiencies as described above in the rejection of claim 2.

Claims 15-19:

In regards to claim 15, Applicant argues (page 9 last paragraph) that *Chuah2 does not teach or disclose one or more control commands employed by a respective network element to establish and manage simultaneous wireless communication sessions of a wireless subscriber unit in a data network.* However, Examiner submits that such limitations are taught by Chuah; as such Chuah in view of Akhtar indeed does teach all the cited limitations.

Examiner respectfully disagrees with the Applicant (page 10 paragraph 2) that Akhtar fails to cure the deficiencies of Chuah; as Chuah indeed does teach the cited alleged deficiencies as described above in the rejection of claim 15.

Examiner respectfully disagrees with the Applicant (page 10 paragraph 3) that claims 16-19 are patentable for the same reasons cited above.

Claims 8 and 9:

Examiner respectfully disagrees with the Applicant (page 10 last paragraph) that Tummala fails to cure the deficiencies of Chuah; as Chuah indeed does teach the cited alleged deficiencies as described above in the rejections of claims 8 and 9.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Salman Ahmed whose telephone number is (571)272-8307. The examiner can normally be reached on 8:30 am - 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hassan Kizou can be reached on (571) 272-3088. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SA
Salman Ahmed
Patent Examiner
5/4/2007

HASSAN KIZOU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600